

### **Remarks**

Applicant respectfully requests reconsideration of this application as amended. Claims 1, 4, 8-11, and 16 have been amended. Claims 25-27 have been cancelled. No claims have been added. Therefore, claims 1-24 are presented for examination.

### **35 U.S.C. §112 Rejection**

Claims 1-10 and 25-27 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically, the Office Action asserts that the claims fail to describe who or what is performing the method steps. Claims 25-27 have been canceled and therefore the 35 U.S.C. §112 rejection of these claims has been obviated. Claims 1-10 have been variously amended to refer to the component performing the individual method steps. As a result, applicant respectfully requests the withdrawal of the 35 U.S.C. §112 rejection.

### **35 U.S.C. §103(a) Rejection**

Claims 1-6, 8, 11-13, and 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Snowden et al. (U.S. Pub. No. 2002/0026332) in view of Intel Internet Authentication Services, Privacy and Security for Health Care Transactions Over the Internet, copyright© 2000, Intel Corporation ("Intel"). Claims 25-27 have been canceled, and therefore the present rejection to these claims has been obviated. Applicant submits that the remaining present claims are patentable over Snowden in view of Intel.

Snowden discloses a secure repository for personal medical records of individuals and families. These electronic records, owned and controlled by the individual, may then be made accessible in selected parts over secured lines to appropriate care providers, insurers, and suppliers. The individual can direct that his or her entire file be transmitted to a doctor or to a hospital emergency room through the use of a coded card or then can direct that their medical information can only be supplied in anonymous, summary form along with data of other insured users to employers/health plan sponsors. (Snowden at Abstract.)

Intel describes Internet Authentication Services (IAS) that offer a managed solution that reduces risk, complexity, and cost, while ensuring state-of-the-art security for online transactions. By taking advantage of IAS, health care service providers may confirm the identities of online visitors to the service provider's web site before granting access to private information. The health care service providers do not have to deploy or maintain complex computing systems for online authentication, as the critical systems reside at a remote location where performance, reliability, and security are maintained. (Intel at pg. 2, cols. 1 & 2.)

Claim 1, as amended, recites:

A method of controlling transfer of health information along a network pathway, the method comprising:

receiving, by an access server on the network pathway, a request for the health information from across an internal network, the request being generated from a portable healthcare device on the network pathway;

immediately determining, by the access server, if a corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information; and

if the corresponding consent is stored, permitting, by the access server, the health information to be immediately acquired by sending the request across an external network to be obtained by a remote site, receiving the health information from the remote site, and forwarding the health information back across the internal network.

Applicant submits that Snowden does not disclose or suggest immediately determining, by the access server, if a corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information, as recited by claim 1. The Office Action states that Snowden discloses “controlling distribution of medical records based on patient consent.” (Office Action at pg. 3, point 3.) However, this control of distribution is performed by the actual patient. The patient further determines to whom and where he or she is sending his or her medical information. (Snowden at Abstract.) Applicant can find no disclosure or suggest anywhere in Snowden of an access server determining if consent is stored for a requestor of health information to access the health information, where the consent is supplied by an owner of the health information.

Applicant further submits that Intel also does not disclose or suggest immediately determining, by the access server, if a corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information. The Office Action states that Intel discloses this feature at page 4, column 1, paragraphs 1 and 2, and also at page 5, column 2, paragraphs 2 and 3. (Office Action at pg. 3, point 3(b).) Yet, these cited portions of Intel only disclose the use of authentication software by health care service providers to authenticate communications with all site visitors to the service provider’s website. The authentication software utilizes digital certificates to authenticate visitors. However, these cited portions do not disclose or suggest the cited feature of claim 1. Moreover, applicant can find no disclosure or suggestion of the cited feature of claim 1 anywhere in Intel.

As neither Snowden nor Intel individually disclose or suggest immediately determining, by the access server, if a corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information, any combination of Snowden and Intel also does not disclose or suggest such a feature. Although Snowden discloses the use of patient control of medical information distribution, this distribution is done entirely under the control of the patient; the patient actually approves and distributed the information himself. Neither Snowden nor Intel disclose immediately determining *by an access server* if a corresponding consent is stored *for a requestor of health information to access the health information* (compared to the patient distributing the information) where the consent is provided by an owner of the health information. Therefore, claim 1, as well as its dependent claims is patentable over Snowden in view of Intel.

Independent claim 11 also recites, in part, a search engine of a health information access server to determine if a corresponding consent is stored in the database for the requested health information, wherein the consent is for the user to access the health information and the consent is provided by an owner of the health information. As discussed above, Snowden in view of Intel does not disclose or suggest such a feature. Therefore, claim 11, as well as its dependent claims, is patentable over Snowden in view of Intel.

Claims 16-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Snowden et al. in view of Intel Internet Authentication Services, Privacy and Security for Health Care Transactions Over the Internet (“Intel”) and further in view of Killcommons et

al. (U.S. Patent No. 6,424,996). Applicant submits that the present claims are patentable over Snowden and Intel in view of Killcommons.

Killcommons discloses a medical information transfer server. The server is adapted to store multimedia medical data and includes a data interface for acquiring the medical data; a storage unit coupled to the data interface and configured to receive and store the medical data; and a user interface for viewing the medical data. (Killcommons at col. 3, ll. 58-64.)

Claim 16, as amended, recites:

A computer accessible medium having stored therein a plurality of sequences of executable instructions, which, when executed by a processor, cause the system to:

process a request for the health information received from across an internal network, the request being generated from a portable healthcare device on the internal network;

immediately determine, by an access server on the internal network, if an corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information; and

if the corresponding consent is stored, permit the health information to be immediately acquired by sending the request across an external network to a remote site, receiving the health information from the remote site, and forwarding the health information back across the internal network.

As discussed above, Snowden in view of Intel does not disclose or suggest immediately determine, by an access server on the internal network, if an corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information, as recited by claim 16. Applicant further submits that Killcommons does not disclose or suggest such a feature. The Office Action acknowledges this when stating “Killcommons fails to disclose...immediately determine if an corresponding consent is stored.” (Office

Action at pg. 13, point 24(b)). Therefore, Killcommons does not disclose or suggest the cited feature of claim 16.

As neither Snowden, Intel, or Killcommons individually disclose or suggest immediately determine, by an access server on the internal network, if an corresponding consent is stored, wherein the consent is for a requestor of the health information to access the health information and the consent is provided by an owner of the health information, any combination of Snowden, Intel, and Killcommons also does not disclose or suggest such a feature. Therefore, claim 16, as well as its dependent claims, is patentable over Snowden and Intel in view of Killcommons.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Snowden et al. in view of Intel Internet Authentication Services, Privacy and Security for Health Care Transactions Over the Internet in view of the Background of the Invention. Applicant submits that the present claim is patentable over Snowden and Intel in view of the Background of the Invention. Claim 7 depends from independent claim 1 and necessarily includes its limitations. As discussed above, claim 1 is patentable over Snowden in view of Intel. The Background of the Invention does not remedy the defects of Snowden and Intel in light of claim 1. Therefore, claim 7 is patentable over Snowden and Intel in view of the Background of the Invention.

Claims 9, 10, 14 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Snowden et al. in view of Intel Internet Authentication Services, Privacy and Security for Health Care Transactions Over the Internet and further in view of Wong et al. (U.S.

Patent No. 6,260,021). Applicant submits that the present claims are patentable over Snowden and Intel in view of Wong. Claims 9, 10, 14, and 15 variously depend from independent claims 1 and 11, and necessarily include their limitations. As discussed above, claims 1 and 11 are patentable over Snowden in view of Intel. Wong does not remedy the defects of Snowden and Intel in light of claims 1 and 11. Therefore, claims 9, 10, 14, and 15 are patentable over Snowden and Intel in view of Wong.

Claims 23 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Snowden et al. in view of Intel Internet Authentication Services, Privacy and Security for Health Care Transactions Over the Internet and further in view of Killcommons et al. and further in view of Wong et al. Applicant submits that the present claims are patentable over Snowden and Intel in view of Killcommons and Wong. Claims 23 and 24 depend from independent claim 16 and necessarily include its limitations. As discussed above, claim 16 is patentable over Snowden and Intel in view of Killcommons. Wong does not remedy the defects of Snowden and Intel in view of Killcommons in light of claim 16. Therefore, claims 23 and 24 are patentable over Snowden and Intel in view of Killcommons and Wong.

Applicant respectfully submits that the rejections have been overcome and that the claims are in condition for allowance. Accordingly, applicant respectfully requests the rejections be withdrawn and the claims be allowed.

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.


Applicant respectfully petitions for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension.

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: April 20, 2006

  
\_\_\_\_\_  
Ashley R. Ott  
Reg. No. 55,515

12400 Wilshire Boulevard  
7<sup>th</sup> Floor  
Los Angeles, California 90025-1026  
(303) 740-1980